AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Detective Jason Maucere, being duly sworn, depose and state:

INTRODUCTION

1. I am a Detective with the Hamilton County Sheriff's Office (HCSO) and am currently acting as a Task Force Officer with the United States Department of Homeland Security Homeland Security Investigations (HSI). I have been a Law Enforcement Officer since June of 2009. I graduated from the Tennessee Law Enforcement Training Academy in 2007 and have had further specialized training in the field of criminal investigations. I hold a Bachelor of Science Degree from Jacksonville University in Jacksonville, Florida, since 2006, and I hold a Master's Degree in Criminal Justice from Boston University since 2009. I have been assigned to multiple divisions during my tenure with the HCSO: as a Deputy Sheriff with the Patrol Division, as a Detective with the Fugitive / Criminal Warrants Division, and as a Detective with the Criminal Investigation Division.

2. I have specialized training and experience in investigating (among other offenses) sex crimes and crimes against children including child sexual abuse, sexual exploitation of minors and child pornography, solicitation of minors by electronic means, trafficking of minors for a commercial sex act, and kidnapping. I have worked joint investigations with local, state, and federal agencies, which have led to the successful prosecution and conviction of persons in Tennessee and federal courts. I am authorized to seek and execute warrants issued under the authority of the United States and have executed or helped execute numerous search and seizure warrants related to child exploitation. Through my training and experience with HSI, I am familiar with the specialized terminology, procedures, and processes referenced in this Affidavit.

3. The statements contained in this Affidavit are based on my personal observations,

my training and experience, as well as information obtained from other law enforcement officers and witnesses. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation.

4. I make this affidavit in support of a search warrant to search the following electronic devices:

A. One (1) Black Apple Watch – Series 6, listed under HCSO property evidence number PE22-02303 (Owner: Johnathan Salazar)

B. One (1) Black Apple iPhone with SIM Card, listed under HCSO property evidence number PE22-02306 (Owner: Johnathan Salazar)

C. One (1) Black Google Android Phone with SIM Card, listed under HCSO property evidence number PE22-02304 (Owner: Johnathan Salazar)

D. One (1) Black Cricket Phone, listed under HCSO property evidence number PE22-02305 (Owner: Johnathan Salazar)

E. One (1) Black 1+ Phone, listed under HCSO property evidence number PE22-02307 (Owner: Johnathan Salazar)

F. One (1) Green Apple iPhone with SIM Card, listed under HCSO property evidence number PE22-02308 (Owner: Margaret Salazar)

(collectively referred to as the SUBJECT DEVICES), which are further described below and in **Attachment A**, hereby incorporated into this Affidavit. The SUBJECT DEVICES are currently in the possession of the Hamilton County Sheriff's Office, 6233 Dayton Boulevard, Chattanooga, Tennessee, in the Eastern District of Tennessee. The information to be seized from the SUBJECT DEVICES is described in **Attachment B**, hereby incorporated into this Affidavit.

5. As further described below, there is probable cause to believe that Johnathan SALAZAR violated Title 18, United States Code, Sections 2422(b), **Coercion and enticement**; 2423(a), **Transportation with intent to engage in criminal sexual activity**, 2423(b), **Travel with intent to engage in illicit sexual conduct**, 2251(a) and (e), **Sexual exploitation of children**

(production of child pornography); and 2252A(a)(1), (2), (5)(B) and (b), **Certain activities relating to material constituting or containing child pornography**; and probable cause to believe that contraband, fruits, instrumentalities, and evidence of such violations is contained within the SUBJECT DEVICES.

APPLICABLE LAW

6. Title 18, United States Code, Section 2422(b) states, "Whoever, using the mail or any facility or means of interstate or foreign commerce, . . . knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in . . . any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be [punished]."

7. Title 18, United States Code, Section 2423(a) states, "A person who knowingly transports an individual who has not attained the age of 18 years in interstate or foreign commerce, . . . with intent that the individual engage in . . . any sexual activity for which any person can be charged with a criminal offense, shall be [punished]."

8. Title 18, United States Code, Section 2423(b) states, "A person who travels in interstate commerce . . . with a motivating purpose of engaging in any illicit sexual conduct with another person shall be [punished]."

9. Title 18, United States Code, Section 2251(a) and (e) states, "Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in . . . or who transports any minor in or affecting interstate or foreign commerce . . . with the intent that such minor engage in[] any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct [or attempts to do so], shall be punished as provided under subsection (e) of this section, if such person knows or

has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed."

10. Title 18, Unites States Code, Section 2252A(a)(1)-(2) and (b)(1) states, "(a) Any person who—(1) knowingly mails, or transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography; [or] (2) knowingly receives or distributes—(A) any child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or (B) any material that contains child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer," or attempts or conspires to do so, "shall be [punished]."

11. Title 18, Unites States Code, Section 2252A(a)(5)(B) and (b)(2) states that any person who "knowingly possesses, or knowingly accesses with intent to view, any . . . material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have

been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer," or attempts or conspires to do so, "shall be [punished]."

PROBABLE CAUSE

12. As further set forth below, HCSO and HSI Chattanooga have been investigating 32-year-old Johnathan Lucino Salazar ("Salazar" or "subject," prior to his positive identification), a resident of Texas, for multiple child exploitation offenses arising out of his course of conduct with a 15-year-old girl ("Minor Victim 1")[1] in Tennessee and other states between at least May and June of 2022. The investigation to date has shown that Salazar met Minor Victim 1 on the social media platform Snapchat in May 2022 and had been grooming her to engage in sexual activity, including by paying money to Minor Victim 1 via Cash App, sending sexually explicit videos of himself to Minor Victim 1, and soliciting Minor Victim 1 to send sexually explicit videos of herself to him. In early June 2022, Salazar traveled from Texas in order to meet Minor Victim 1 in Tennessee and bring her back to Texas with him. After Salazar picked up Minor Victim 1 in his truck on June 2, 2022, and Minor Victim 1 was reported missing, law enforcement launched an intensive investigation that, through tracking of Minor Victim 1's and Salazar's cell phones (among other investigative techniques), was able to locate Minor Victim 1 and Salazar in a hotel room in Meridian, Mississippi. Also found in the hotel room and in Salazar's truck, which was in the hotel parking lot, were the SUBJECT DEVICES.

13. On June 2, 2022, at 17:07 hours, Deputy Shadwick, Deputy Turner, and Sergeant Miller of the HCSO responded to a residence within the Eastern District of Tennessee on report of a missing juvenile. Upon arrival, the deputies spoke with the reporting party, who stated her 15-

[1] Minor Victim 1's identity is known to law enforcement but is omitted here to protect her privacy. *See generally* 18 U.S.C. § 3509(d).

year-old daughter, Minor Victim 1, was missing. While on scene, deputies learned that another family member had contacted Minor Victim 1 via her cellphone and that Minor Victim 1 had told the family member that she was in Alabama and was safe but did not plan on coming home. Minor Victim 1 also stated to her family member that she was with a male she had met on Snapchat but would not give the male's name. Minor Victim 1 then told her family to check the mailbox. Minor Victim 1's mother then checked the mailbox and found a handwritten letter from Minor Victim 1 inside the mailbox, which read, in part, *"I'm going to be safe where I'm going I promise and might keep contact sometimes. . . . You don't need to call anyone because I know I'll be safe and know who to call if I ain't. Ya'll don't have to worry. I can give them your number even tho I'm safe."*

14. Due to the reported runaway missing juvenile, Sergeant Miller directed Hamilton County Dispatch to obtain location pings for Minor Victim 1's cellular phone (i.e., to determine the estimated current location of the cellphone via GPS data or cell tower triangulation from the cellphone provider). At 17:46 hours, Sergeant Miller contacted your Affiant and advised him of the missing juvenile. Sergeant Miller also advised Affiant that Dispatch learned the cellphone provider (Verizon Wireless) was pinging Minor Victim 1's cellphone near Birmingham, Alabama. Minor Victim 1's mother then advised the Deputies she had knowledge of a man named "John," whom she believed lived in Cleveland, Texas, who had sent Minor Victim 1 approximately $500 that day via Cash App. Minor Victim 1's mother stated Minor Victim 1 was attempting to access the money and that Minor Victim 1 had stated she (Minor Victim 1) needed the money that day but would not say why. (Detectives were advised that Minor Victim 1's mother was of the belief the man named "John" was a teenage male, thus not causing her to have suspicion or concern her daughter was being contacted by an older male subject.) Sergeant Miller then advised Affiant about the information of the male subject sending Minor Victim 1 $500 via Cash App. Upon

receiving the information regarding the missing juvenile receiving $500 via Cash App, Affiant determined this incident was not likely a simple runaway juvenile and that the evidence of the cellular ping locations in Alabama with the $500 cash gifts highly indicated sexual exploitation of a child and a child abduction. Affiant then notified CID Lieutenant Harvey, and emergency protocols were initiated.

15. Detective Maucere (Affiant) and Detective Terry began an intense investigation to identify the subject who had taken Minor Victim 1 out of Tennessee. Detective Terry was able to work with Minor Victim 1's mother to obtain the Cash App information and dates of the cash transfers from the subject to Minor Victim 1. Detective Terry determined the cash transfers were being sent from a subject named "Johnny" with the Cash Tag $jkashu7 and determined eight separate cash transfers from the subject to Minor Victim 1 occurring between May 17, 2022, and May 27, 2022, in a total dollar amount of $535.00. Detective Terry also determined two failed Cash App cash transfers occurred on May 16, 2022, and May 17, 2022, in the amounts of $15.00 each.

a. The first transaction occurred May 16, 2022, at 23:52 hours in the amount of $15.00 (failed transaction) with the caption: *"For te amo."* I know that "te amo" means "I love you" in Spanish.

b. The second transaction occurred May 17, 2022, at 12:07 hours in the amount of $15.00 (failed transaction) with the caption: *"For hello."*

c. The third transaction occurred May 17, 2022, at 23:20 hours in the amount of $15.00 with the caption: *"For mi amor."* I know that "mi amor" means "my love" in Spanish.

d. The fourth transaction occurred May 20, 2022, at 14:02 hours in the amount of $20.00 with the caption: *"For lunch."*

e. The fifth transaction occurred May 21, 2022, at 16:14 hours in the amount of $50.00 with the caption: *"For snack of anything Te AMO MI AMOR."*

f. The sixth transaction occurred May 22, 2022, at 21:12 hours in the amount of $150.00 with the caption: *"For don't argue for u and* [another female's name] *I love y'all my girls."*

g. The seventh transaction occurred May 23, 2022, at 04:50 hours in the amount of $50.00 with the caption: *"For snacks and new outfit for baby girl."*

h. The eighth transaction occurred May 27, 2022, at 14:47 hours in the amount of $150.00 with the caption: *"For so you can buy what u want mi amor I'm sorry."*

i. The ninth transaction occurred May 27, 2022, at 15:59 hours in the amount of $50.00 with the caption: *"For for gas or anything babe."*

j. The tenth transaction occurred May 27, 2022, at 21:19 hours in the amount of $50.00 with the caption: *"For be safe walking the beach at night my love."*

16. Detective Terry was able to work with Minor Victim 1's mother to obtain multiple screenshots from conversations between Minor Victim 1 and the subject via Snapchat. More specifically, Minor Victim 1's mother was able to use her own Snapchat account, which had been "friends" with Minor Victim 1's Snapchat account, to connect to Minor Victim 1's Snapchat account, which in turn shared account information with Minor Victim 1's mother's account. Minor Victim 1's mother was able to take screenshots of conversations she saw in Minor Victim 1's account and to share these with Detectives. One of the screenshots contained a full body "selfie" photo depicting a Hispanic male (with his face obscured by the camera) whom Affiant later identified as Jonathan Salazar. Detectives also reviewed Snapchat messages between Minor Victim 1 and the subject, depicted in Snapchat as "John" with display name "Johnnyboy6", which occurred on June 2, 2022, and which clearly indicated the subject's arrival in Tennessee and intent to pick up Minor Victim 1 when no other individuals were around and transport Minor Victim 1 away from Tennessee. The Snapchat messages included the following:

John: *"my love I'm almost yo* [sic] *you I would never leave you."*

John:	*"I'm hear* [sic] *do I wait at the church . . . ? Im gonna drive around but where do I get in the driveway I don't know which road to turn to I turn to* I'm going to wait at the gas station call me okay"*
John:	*"Do u want me to drive in there I'll just wait and listen to what u tell me to do love"*
Minor Victim 1:	*"Ok well hold on"*
John:	*"Okay love"*
. . . .	
Minor Victim 1:	*"Haha yea also I don't feel comfortable leaving* [name] *out here in this is about to storm"*
John:	*"Bring him with u"*
Minor Victim 1:	*"I will idk* [I don't know] *when I can go though unless they stay in the rooms"*
John:	*"I know it's okay love I'll be here chilling . . . "*
Minor Victim 1:	*"Ok I'm sorry. . . "*
John:	*"Don't be sorry love it's okay . . . "*
Minor Victim 1:	*"Want if we gotta wait tilt tn* [tonight] ... *Not saying we might not have to through What*"*
John:	*"I can wait till tonight it not a problem love but if u have chance to lmk* [let me know]*"*
Minor Victim 1:	*"Ok I'm sorry"*
John:	*"It's okay"*
Minor Victim 1:	*"You've been waiting like an hour"*
John:	*"I'll wait forever if I have to for u"*
Minor Victim 1:	*"Your work said you gotta be back Friday"*
John:	*"I know but I'm cool with the bosses so they understand plus we have ppl to cover me"*

Minor Victim 1: *"If they wasn't outside I would be able to go but* [name]*'s outside"*

John: *"I'll wait okay love"*

Minor Victim 1: *"I'm sorry"*

John: *"Don't sorry everything will be okay I'll wait love I want you to be happy"*

Minor Victim 1: *"Hi"*

17. Affiant and Detective Terry continued the investigation, and Minor Victim 1's mother advised Detective Terry that she found an old cellphone belonging to Minor Victim 1 and had looked in it and discovered the phone number 361-676-4721 associated with "Johnny" in the phone and believed this was the subject. At 20:48 hours, still on June 2, 2022, Affiant made contact with Verizon Wireless (which Affiant had determined was the provider of that cellphone number via an open-source database known as CLEAR) and requested assistance from the Verizon Security Assistance Team, due to the exigent circumstances involved in this case, with initiating an emergency disclosure request for subscriber data and GPS location data for phone number 361-676-4721, pursuant to an 18 U.S.C. § 2702 exception. Verizon responded with the GPS coordinates for the cellphone number, which indicated the phone (and thus likely the subject) was in Meridian, Mississippi. At 21:10 hours, Hamilton County Dispatch advised that it had received an updated ping location for the Minor Victim 1's phone and that this location was now also in Meridian, Mississippi. Detective Terry was also then advised by Minor Victim 1's mother that Minor Victim 1's mother had called Minor Victim 1 on the phone and spoken with her briefly; Minor Victim 1 advised her mother that she was in a hotel room; however, she would not tell her mother where. At 22:20 hours, Affiant again contacted Verizon Wireless and requested a second emergency disclosure for locations for Minor Victim 1's phone number in addition to the subject's

phone number 361-676-4721. Verizon conducted an immediate location ping for both phones, and their locations both indicated 201 S. Frontage Road, Meridian, Mississippi, within an approximate 700-meter radius; however, the phone pings showed both phones to be within only two meters of each other, indicating the subject and Minor Victim 1 were together. Detective Terry contacted the Meridian Police Department, who was already checking the area due to an earlier alert by Hamilton County Dispatch, and gave them the updated information along with possible vehicle information for the subject, as set forth below.

18. In speaking with representatives of Verizon Wireless for the emergency disclosure request, Affiant learned that the subscriber for phone number 361-676-4721 was Johnathan Salazar with an address in Victoria, Texas. Affiant used this name and specific address to conduct a search utilizing CLEAR databases and found the likely identity, including date of birth and social security number, along with possible vehicle information, for the subject. Affiant then utilized the information from CLEAR and was able to positively identify the subject as Johnathan Lucino Salazar via NCIC and a Texas driver's license including a photo. Affiant was also able to identify 3 motor vehicles associated with Johnathan Salazar to include a 2018 Ford F-150 (TX TAG: RNG8134 / VIN: 1FTEW1CG8JKF54041), a 2016 Honda Fit (TX TAG: JKV6520 / VIN: JHMGK5H50GX003325), and a 2018 Honda unknown model (TX TAG: NBX9250 / VIN: 2HGFC2F52JH554820), and this information was provided to the Meridian Police Department, who then attempted to locate these vehicles in the area of S. Frontage Road, which was the location of a number of hotels.

19. Detective Terry worked with Minor Victim 1's mother to locate Minor Victim 1 via Snapchat. Minor Victim 1's mother was able to re-activate her profile and was then able to sync her profile with Minor Victim 1's Snapchat profile, as described above, in an attempt to get

Minor Victim 1's location information. On June 3, 2022, at approximately 00:05 hours, Minor Victim 1's mother contacted Detective Terry and provided him with Minor Victim 1's location via Snapchat. Minor Victim 1's mother was able to view the location of Minor Victim 1 via Snapchat's "location sharing" feature, which allows Snapchat users to view each other's GPS locations while using the platform, if the specific users have given certain permissions within the Snapchat application to allow the social media platform to access and share this data. Detective Terry then checked Minor Victim 1's location via the use of Snapchat and found her location was at 519 Azalea Drive, Meridian, Mississippi 39301, which was the address of the hotel Tru by Hilton. Upon receipt of this information, Detective Terry contacted the Meridian Police Department and updated them on the exact whereabouts of Minor Victim 1, and the Meridian Police Department responded to this address. At 00:10 hours, the Meridian Police Department recovered Minor Victim 1 in a hotel room at the Tru by Hilton and arrested Salazar, who was found with her in the hotel room (along with two other adult females: Margaret Salazar—the subject's mother—and her friend). The Meridian Police Department also advised HCSO that they had located Salazar's gray 2018 Ford F-150 in the parking lot of the hotel. Affiant and Detective Terry then responded to Meridian, Mississippi, to recover Minor Victim 1 and to interview Salazar.

20. On June 3, 2022, at 06:04 hours, Affiant and Detective Terry interviewed Minor Victim 1 at the Meridian Police Department. Minor Victim 1 positively identified Salazar as the person who had taken her from Tennessee to Mississippi by his Texas driver's license photo. Minor Victim 1 stated she had met Salazar over Snapchat several weeks earlier. Minor Victim 1 stated Salazar had planned to come take her from Tennessee and bring her to his home in Texas

and that he had told her he was 19 or 20 years old.[2] Minor Victim 1 stated Salazar had Facetimed her in the morning of June 2, 2022, and had told her he was on his way and that they had been in contact while he was en route. Minor Victim 1 stated Salazar had told her not to tell her mom that he was coming to pick her up. Minor Victim 1 stated she was surprised when she first saw Salazar—when he picked her up on June 2, 2022—because he had turned out to be older than he had said. Minor Victim 1 also stated Salazar told her they could sleep at a hotel then go back to Tennessee if she wasn't comfortable. Minor Victim 1 stated they went to the Tru by Hilton hotel in Meridian, where she met the two other adult females, who were inside the hotel room. Minor Victim 1 further stated that she slept in the same bed as Salazar (the one located away from the window in the hotel room), though she stated both she and Salazar were clothed and denied any sexual activity occurred in the hotel room. Affiant asked Minor Victim 1 if Salazar had asked her for nude photos or photos that were suggestive or if Salazar had paid her for nude photos, and Minor Victim 1 denied these things had occurred, although she acknowledged that she had sent photos of herself with clothes on and stated that Salazar had sent her money via Cash App. Minor Victim 1 stated Salazar told her he had a lot of money that he had inherited from his father. Minor Victim 1 also stated to detectives that Salazar had asked her if she wanted to go to Texas and that she had said "yes" to this question. Minor Victim 1 stated she planned to stay in Texas for one week and then she believed Salazar would drive her back to Tennessee. Minor Victim 1 stated Salazar had told her that he loved her; however, she did not think she was in a "relationship" with Salazar. Minor Victim 1 further told detectives that Salazar knew she was 15 years old.

[2] Minor Victim 1 later stated to Affiant and Detective Terry, following the formal interview, that Salazar told her he was 17 years old when he first had contacted her on Snapchat.

21. On June 3, 2022, at 07:08 hours, Affiant and Detective Terry interviewed Salazar at the Meridian Police Department. Prior to questioning Salazar, Affiant provided Salazar with a Miranda warning and asked if he understood his rights and wished to speak with police regarding his arrest and what had occurred with Minor Victim 1. Salazar waived his rights and agreed to speak with police. During the interview, Salazar admitted to driving from his home in Victoria, Texas, to Tennessee to pick up Minor Victim 1. Salazar stated he had been added by Minor Victim 1 on Snapchat approximately one month ago and he had developed a relationship with her. Salazar told detectives he had fallen in love with Minor Victim 1. Affiant asked Salazar if he had specifically driven from Texas to Tennessee to take Minor Victim 1 back to Texas, and he stated yes to these questions and stated his intention was to take Minor Victim 1 back to his home in Victoria, Texas, to live with him. Salazar then told detectives he knew this was wrong and admitted he knew Minor Victim 1 was 15 years old. Salazar also admitted to detectives he had lied to Minor Victim 1 about his age: he had told her he was 20 when they first communicated over Snapchat, and it was not until June 2, 2022, that he told her he was older. Affiant asked Salazar about the sleeping arrangements at the hotel, and Salazar stated he slept in another bed than the one Minor Victim 1 was in (contrary to the statement made by Minor Victim 1 during her interview). Salazar admitted to paying Minor Victim 1 via Cash App over several weeks, in the total amount of $537.00. When Affiant asked Salazar if he had ever exchanged any sexually explicit material with Minor Victim 1, Salazar admitted he had masturbated himself on video over Snapchat with Minor Victim 1 watching and that he had watched Minor Victim 1 masturbate herself on video over Snapchat. Salazar further acknowledged that he had used Facetime to communicate with Minor Victim 1 before meeting her in person. Salazar also stated that, when his mother had learned he was traveling to pick up a female in another state, she began tracking

him using her cellphone and the "360" app, that she had shown up at the hotel, and that she met Minor Victim 1 there, though she had not known that Minor Victim 1 was a minor in advance.[3]

22. Following the recorded interview, Affiant asked Salazar for permission to search his vehicles, and Salazar gave verbal permission to perform a search of the vehicles. Salazar also provided a passcode for his cellphone to detectives during the recorded formal interview.

23. Also following the formal interview with Salazar, on June 3, 2022, Salazar approached Affiant in a holding cell and made a spontaneous utterance to Affiant that detectives would find several $600.00 cash deposits to his bank account that looked suspicious but were from his employer (Donut Palace in Victoria, Texas), who paid him in cash. In my training and experience, such cash payments may be indicative of payments made by criminal organizations, which tend to pay members in cash to avoid a paper trail, or by other individuals seeking to obtain and exploit a child without a paper trail. Salazar's employment activities and payments remain under investigation.

24. The Meridian Police Department found and seized numerous cell phones in the hotel room during Salazar's arrest—including three determined to belong to Salazar, one belonging to his mother (i.e., one of the other adult hotel room occupants), and one belonging to Minor Victim 1—and one additional cellphone belonging to Salazar was found later that day (June 3, 2022) during a vehicle search by detectives, as further described below. I know, in my training and experience, that multiple cellular phones can be indicative of criminal activity, including but not limited to human trafficking and other child exploitation. Individuals associated with organized crime and / or other criminal activity often have, in common practice, multiple cellular

[3] Later review of Minor Victim 1's phone, pursuant to a consent search, revealed messages between Salazar's mother and Minor Victim 1 while Salazar and Minor Victim 1 were en route to the hotel.

phones with which to communicate with other criminal actors, which are used to provide anonymity to those involved. Phone numbers, SIM cards, and actual cellular phones are oftentimes changed periodically in an attempt to elude tracking by law enforcement. Law enforcement also observed an Apple Watch—which, as set forth below, I know from my training and experience can also contain evidence of criminal activity, including the location and activities of an offender during the relevant time frame—belonging to Salazar in the hotel room. Accordingly, detectives seized the four cell phones and one Apple Watch belonging to Salazar (SUBJECT DEVICES A through E), in addition to Minor Victim 1's cellphone (which is not listed in Attachment A) and Salazar's mother's cellphone (SUBJECT DEVICE F). Minor Victim 1 later disclosed to detectives, during the ride back to Tennessee, that Salazar had also purchased her a new cellphone, which, from my training and experience, is indicative of criminal activity including human trafficking and of intent to isolate the victim from her family and from any chance of contacting police and from any tracking by law enforcement authorities. From investigation to date, I believe the cellphone provided by Salazar to Minor Victim 1 is one of the SUBJECT DEVICES.

25. On June 3, 2022, at approximately 10:30 hours, Affiant and Detective Terry responded to the Tru by Hilton with a detective with the Meridian Police Department and conducted searches of the 2018 Ford F-150 and 2016 Honda Fit, which were parked in the hotel parking lot. Salazar had previously given detectives verbal consent to search his vehicles, which included the 2018 Ford F-150 and 2016 Honda Fit. During the search of the 2018 Ford F-150, detectives seized a cellphone (one of the SUBJECT DEVICES) which was located in a locked center console of the vehicle.

26. On June 3, 2022, Salazar waived extradition from Mississippi to Tennessee on a hold for pending felony criminal charges for violations of Tennessee law (described on the Waiver

of Extradition as Aggravated Kidnapping (TCA 39-13-304 / Class B Felony), Trafficking for Commercial Sex Act (TCA 39-13-309 / Class B Felony), and Solicitation of a Minor (TCA 39-13-528 / Class E Felony)). Salazar was then transported to the Kemper Neshoba Regional Correctional Facility to await extradition to Tennessee. Also on June 3, 2022, Affiant transported the SUBJECT DEVICES from Mississippi to Tennessee where they were secured and have remained secured at the Hamilton County Sheriff's Office West Annex located at 6233 Dayton Boulevard, Chattanooga, Tennessee 37343, for safekeeping and for future examination pursuant to a search warrant. On June 5, 2022, Affiant charged Salazar, by complaint, with the Tennessee state offenses of Aggravated Kidnapping (TCA 39-13-304 (a) (1) / Class B Felony), Trafficking a Person for a Commercial Sex Act (TCA 39-13-309 (a) (1) & (a) (2) / Class B Felony), Solicitation of a Minor under 18 Years of Age (TCA 39-13-528 / Class C Felony), Solicitation of a Minor to Observe Sexual Conduct (TCA 39-13-529 section (a) / Class B Felony), and Solicitation of a Minor to Observe Sexual Conduct (TCA 39-13-529 section (b)(1) / Class E Felony). On June 12, 2022, Salazar was extradited from Mississippi to Tennessee on arrest warrants for the above criminal charges and was transported by the Hamilton County Sheriff's Office Fugitive Division to the Hamilton County Jail / Silverdale Detention Center, where he remains in custody.

27. On approximately July 15, 2022, HSI Forensic Examiner Steven Burns completed a forensic cellular data extraction (also known as a "phone dump") on a Moto G Pure smartphone which was positively identified as the smartphone belonging to Minor Victim 1 and found on her person in the hotel room on June 3, 2022 (this phone is not listed in Attachment A). Minor Victim 1's mother signed a consent to search form authorizing law enforcement to conduct the forensic examination of the phone's digital data. Following the cellular data extraction, Affiant and Detective Terry reviewed SMS text messages and Snapchat instant messages between Salazar and

Minor Victim 1 that were in the phone. More specifically, upon review of the SMS text messages, detectives discovered conversations between both parties initiating on May 18, 2022, and continuing through May 31, 2022. Detectives observed that on May 30, 2022, at 19:37 hours, Minor Victim 1 told Salazar that she was 15 years old: *"And your family [sic] you said I was 18. I'm 15."* Detectives also found messages of a sexual nature, including on May 28, 2022, from 22:53 hours through 22:55 hours, when Minor Victim 1 asked, *"Why you not cum for me????"* and Salazar replied, *"I'm still doing it but I was texting u on Here I'll cum for u rn [right now] okay."*

28. Detectives reviewed the Snapchat instant messages between Salazar and Minor Victim 1 and observed a large portion of the Snapchat messages contained sexual content. The Snapchat instant message thread occurred between May 13, 2022, and June 3, 2022, and includes 2,296 Snapchat messages. On a Snapchat instant message thread occurring on May 13, 2022, from 23:10 hours through 23:19 hours, Salazar demonstrated his knowledge that Minor Victim 1 was a 15-year-old minor and that he was interested in engaging in sexual activity with Minor Victim 1:

Minor Victim 1:	*"Show your face"*
Salazar:	*"Not yet okay I'll give u ever thing but give me time on that okay How old are u first"*
Minor Victim 1:	*"Don't leave tho Promise? Im 15 go if ya want im sorry for bothering you"*
Salazar:	*"I won't leave I promise I'll stay here for u but I'm 20 tho Only if ur okay with that"*
Minor Victim 1:	*"Ok that's fine"*
Salazar:	*"Are u sure? U like older guys?"*
Minor Victim 1:	*"Mhm"*

Salazar: *"Ur right only 5 yrs So u want to be more than friends than?"*

Minor Victim 1: *"No stay what we are rnm"*

Salazar: *"Okay let just be friends than With benefits I'm from tx tho"*

29. Detectives continued examining the Snapchat instant messages and observed continuous strong sexually explicit text content between Salazar and Minor Victim 1 following Minor Victim 1 advising him she is a 15-year-old minor. For example, Snapchat instant messages on May 14, 2022, from 01:55 hours through 01:59 hours, include the following:

Minor Victim 1: *"I be on my period...But still wanna get fucked the shit out of"*

Salazar: *"And I wanna be the one to do that yk...I wish I was there rn so I could"*

Minor Victim 1: *"I'm on my period tho"*

Salazar: *"I don't care it's just blood...I wanna make u feel happy yk...And I'll do it raw"*

Affiant observed strong sexual content continued throughout the course of the Snapchat instant messages, which included Salazar talking to Minor Victim 1 about his penis, masturbation, ejaculating, and having vaginal, anal, and oral sex with Minor Victim 1; references to numerous sexually explicit photos and videos depicting and shared between Salazar and Minor Victim 1; communication with Minor Victim 1 about making sex videos with her for extra money; and references to plans to travel with Minor Victim 1 and have sex with her during their travels. Affiant also observed that both Salazar and Minor Victim 1 referenced numerous sexually explicit videos and photos of themselves which they were sending each other in Snapchat "snaps" and referenced engaging in mutual masturbation via FaceTime video chat.[4]

[4] I know from my training and experience that videos and photos sent over Snapchat—unlike the text of the messages—are not automatically saved to the user's device. Law enforcement did not find the referenced Snapchat

30. From my training and experience in cases related to child sexual abuse or child sexual exploitation, I am aware that child sexual abuse material (CSAM, commonly known as child pornography) is often saved and recorded by an offender for later viewing and further sexual gratification of the offender. From my training and experience, I have knowledge that offenders who engage in live video calls or live video chatrooms with child victims often record the live sessions in order to continue to view the sex act to attain further sexual gratification. From my training and experience, I also have knowledge that offenders who create or record CSAM often share this content with other criminals who exploit children. Based upon what was discovered in the SMS text messages and Snapchat instant messages, I believe probable cause exists to believe that videos and photographs of Minor Victim 1 engaged in sexually explicit conduct, and/or other evidence of the sharing of such videos and images, are on the SUBJECT DEVICES. I also believe probable cause exists that the SUBJECT DEVICES contain further evidence of Salazar's enticement of Minor Victim 1 and intent to travel in interstate commerce and transport Minor Victim 1 in interstate commerce with the intent to engage in criminal sexual activity (including but not limited to intercourse) with Minor Victim 1.

31. The SUBJECT DEVICES are currently in storage at the Hamilton County Sheriff's Office, located at 6233 Dayton Blvd, Chattanooga, Tennessee, in the Eastern District of Tennessee. In my training and experience, I know that the SUBJECT DEVICES have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same

---

videos/photos in Minor Victim 1's cellphone. However, as further set forth in this Affidavit, I know that a user can manually save such videos/photos, and, from my training and experience, I know that many individuals with a sexual interest in children and child pornography will save such videos and photos to their own device(s).

state as they were when the SUBJECT DEVICES first came into the possession of law enforcement.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ENGAGE IN THE SEXUAL EXPLOITATION OF CHILDREN

32. Based on my previous experience related to child exploitation investigations and child sexual abuse investigations (including but not limited to child pornography investigations), and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals who engage in the sexual exploitation of children (including those who entice and coerce children to engage in sexual activity and who produce, transport/receive, and possess child pornography):

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses in person, photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. In some instances, these depictions show the individual's own sexual activity with children. Further, such individuals may use these materials to lower the inhibitions of children that they are attempting to seduce, to arouse the selected child victim, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their "hard copies" of child pornographic material, that is, their films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain photos, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer, cell phone, or other electronic storage devices (e.g., hard drives or USB drive). These collections are often maintained for years and are kept close by, usually at the individual's residence (or other location where staying), inside the individual's vehicle, or on the individual's person, to enable the individual to view the collection, which is valued highly. Although it is possible, a person who has this type of material is not likely to destroy the collection, including during moves.

e. Such individuals also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors and child exploitation offenders; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography and exploitation.

f. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Such individuals frequently retain records of their child exploitation and child pornography activities for long periods of time, particularly when they are involved in ongoing criminal conduct. Offenders who engage in child exploitation and child pornography often do so for extended periods of time spanning years, and due to the nature of the crime retain evidence and records of their activities for many years. Based on my experience, the passage of long periods of time will not remove the possibility that the evidence of the crimes will still remain. The evidence may also be innocuous at first glance (e.g., financial, credit card and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, telephone and address directories, check books, videotapes and photographs, utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone and pager bills, keys to safe deposit boxes, packaging materials, computer hardware and software), but have significance when considered in light of other evidence. These persons may no longer realize they still possess the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. These persons may also be under the mistaken belief that he/she has deleted, hidden or further destroyed any computer-related evidence, but this information may be retrievable by a trained forensic computer expert.

h. Individuals involved in child exploitation and child pornography and/or their associates frequently take, or cause to be taken, photographs or videotapes of themselves, their associates, their property, and their product, and maintain those

photographs or videotapes in their residences and within their computer and electronic equipment.

i. Individuals involved in child exploitation and child pornography often travel by car, bus, or other means of transportation, both domestically and to and/or within foreign countries, in connection with their illegal activities in order to meet with victims or coconspirators, and to conduct child exploitation-related activities. Documents relating to such travel, such as calendars, travel itineraries, maps, airline ticket and baggage stubs, frequent use club membership information and records associated with airlines, rental car companies, and/or hotels, airline, hotel and rental car receipts, credit card bills and receipts, photographs, videos, passports, and visas, are often maintained by offenders engaged in child exploitation and child pornography in their residences, stash houses, businesses, on their computers/phones and/or in vehicles where they are readily available for use or reference.

j. These persons frequently maintain listings of names, aliases, telephone numbers, pager numbers, facsimile numbers, physical addresses, and email addresses, sometimes encoded and sometimes not encoded, for the purpose of contacting their victims or co-conspirators, and these records are typically maintained on their person or in their residences, stash houses, businesses, and/or vehicles, so they are readily available in order to efficiently conduct their child exploitation- related activities. Moreover, such records are often stored electronically within the memory of telephones, computers, and/or personal digital assistants such as iPhone, Android and other electronic devices.

k. Individuals involved in child exploitation and child pornography frequently utilize cellular telephones, satellite telephones, pagers and text messaging devices,

voicemail or answering machine systems, telephone calling cards, computers, email, and/or personal digital assistants such as "smart" phones in order to communicate with their victims or co-conspirators, and these items are often maintained on their person or in their residences, stash houses, businesses, and/or vehicles where they are readily available. A cellular telephone's memory may contain the telephone number that is assigned to that telephone (which will enable investigators to retrieve records concerning that telephone and analyze those records). In addition, cellular telephones often have internal logs which record the outgoing and incoming calls, including the numbers associated with those calls, and this information can also assist in identifying victims or co-conspirators. Similarly, cellular telephones are commonly used for text messages or other forms of electronic messages and often store the messages, and these messages may provide insight into (a) the nature, extent and methods of child exploitation activities and operations of the offender and co-conspirators; (b) the identities and roles of co-conspirators; (c) the distribution and transfer of photographs, images, videos, and other records involved in those activities; (d) the existence and location of relevant records; (e) the location and source of resources used to finance their illegal activities; and (f) any attempt to hide the identity or location of those involved. In addition, the information in a phone's memory may constitute admissible evidence of the commission of child exploitation-related offenses. Cellular telephones, computers and other electronic storage devices may also include an address book, calendar, and lists of frequently called telephone numbers which may help establish the identities of other individuals who are in frequent contact with the user and involved in child exploitation-related activities. These devices may also include photographs, video recordings and other records of the type described above. Based on my training and

experience, I know that even though individuals involved in child exploitation and child pornography may discontinue use of a telephone, they will sometimes keep the physical phone in their possession and that relevant evidence may still be obtained from the phone.

l. Such individuals often use fake accounts, including those purportedly of minors, to communicate with children they are grooming and/or enticing to engage in sexual activity. It is common for such individuals to send explicit photos of themselves or others along with sexualized conversations in an effort to make the child comfortable with sexual activity.

m. Non-pornographic, seemingly innocuous images of minors are often found on media belonging to child exploitation offenders. Such images are useful in attempting to identify actual minors depicted in child pornography images, or who were otherwise exploited by the offender, that are found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images, or the location of the offender's contact with the minor.

n. In some cases of child sexual exploitation, individuals who exploit children become involved with human trafficking organizations and may be associates or members of criminal street gangs, drug cartels, or organized crime groups who buy and sell children, minors, and adult victims for human slavery or for sexual slavery. Devices and media belonging to individuals who sexually exploit children may contain digital evidence which may help to identify if the subject has been contacted by, working with, paid by, or become involved with a criminal organization that traffics children or adults for financial profit. In these cases, devices and media can be invaluable in identification of criminal contacts,

phone numbers, locations, addresses, bank routing and account numbers, and other identifying information of known criminal organizations.

o. I have reason to believe that Salazar shares the above characteristics common to individuals who sexually exploit children, including those who use the Internet and other means of interstate commerce to engage children in sexual activity and to produce, transport/receive, and possess child pornography, based on the following: as further set forth in this Affidavit, Salazar sent numerous SMS text messages to Minor Victim 1, which reflect a sexual and purportedly romantic relationship with Minor Victim 1 (known in these type of investigations as "grooming," wherein the subject attempts to desensitize and persuade the victim to provide sexually explicit material and/or engage in sexually explicit conduct); Salazar sent numerous Snapchat instant messages where he engaged in sexually explicit conversations with Minor Victim 1 and described wanting to travel to and with the victim and engage in criminal sexual activity with the victim (including but not limited to sexual intercourse), Salazar admitted to exchanging videos of himself and Minor Victim 1 masturbating over Snapchat, and Salazar acted upon his intention to meet Minor Victim 1 by driving from Texas to Tennessee and transporting Minor Victim 1 in interstate commerce until he was stopped by law enforcement in a hotel room with Minor Victim 1.

ELECTRONIC DEVICES AND FORENSIC ANALYSIS

33. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through

radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media

include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most

PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique alphanumeric address used by computers on the Internet. Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. Apple Watch: An Apple Watch is a smartwatch produced by Apple Inc., which is in essence a wearable computer device which runs software known as "watchOS" and interfaces with Apple iPhone software known as "iOS" and interfaces with Macintosh computer software known "macOS." Apple Watch "watchOS" software is able to sync the Apple Watch applications with Apple iPhones and Macintosh computers to perform wireless cellular phone calls, email, instant messages, GPS maps, music play, photo view and storage, Apple Wallet, Apple Pay, and fitness tracking applications. The Apple Watch, when synced, becomes an extension of the applications used on both an Apple iPhone and

Macintosh computer and can display and store digital images, can engage in telecommunications, can send and receive text messages, and can display and store videos which have been created, received, or stored by the Apple iPhone and Macintosh computer.

34. Based on my training, experience, and research, I know that the SUBJECT DEVICES have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA, as well as storage devices. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

35. Based on my knowledge, training, and experience, I know that electronic devices such as the SUBJECT DEVICES can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

36. There is probable cause to believe that things that were once stored on the SUBJECT DEVICES may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space (also known as unallocated data or unallocated space)—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

37. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file

(such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to produce, transport/receive, or possess child pornography, or to entice a minor to engage in sexual activity, the individual's electronic device will generally serve both as an instrumentality for committing the crime and as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

g. Based on my knowledge, training, and experience, I know that electronically stored files, particularly photos and videos, must typically be reviewed by the examiner in order to confirm their contents, because file names can easily and purposefully be misleading and files stored in a way that their true nature is hidden by offenders.

38. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might

expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

39. Manner of execution. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

40. Based on this investigation, I submit there is probable cause for a search warrant authorizing the examination of the SUBJECT DEVICES described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Detective Jason Maucere
Hamilton County Sheriff's Office
HSI Task Force Officer

Subscribed and sworn to before me on August 15, 2022.

HON. CHRISTOPHER H. STEGER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to:

A. One (1) Black Apple Watch – Series 6, listed under HCSO property evidence number PE22-02303

B. One (1) Black Apple iPhone with SIM Card, listed under HCSO property evidence number PE22-02306

C. One (1) Black Google Android Phone with SIM Card, listed under HCSO property evidence number PE22-02304

D. One (1) Black Cricket Phone, listed under HCSO property evidence number PE22-02305

E. One (1) Black 1+ Phone, listed under HCSO property evidence number PE22-02307

F. One (1) Green Apple iPhone with SIM Card, listed under HCSO property evidence number PE22-02308

(collectively the SUBJECT DEVICES), held at the Hamilton County Sheriff's Office (HCSO), located at 6233 Dayton Blvd, Chattanooga, Tennessee, in the Eastern District of Tennessee.

This warrant authorizes the forensic examination of the SUBJECT DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED

All records, located within the SUBJECT DEVICES listed in Attachment A, that constitute contraband or evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 2422(b), **Coercion and enticement**; 2423(a), **Transportation with intent to engage in criminal sexual activity**, 2423(b), **Travel with intent to engage in illicit sexual conduct**, 2251(a) and (e), **Sexual exploitation of children** (production of child pornography); and 2252A(a)(1), (2), (5)(B) and (b), **Certain activities relating to material constituting or containing child pornography**; including:

1. Images or visual depictions of child pornography, as that term is defined in 18 U.S.C. § 2256(8).

2. Images and videos of child erotica (i.e., children engaged in sexually suggestive poses or settings that do not meet the definition of child pornography).

3. Information, correspondence, records, documents, or other materials constituting evidence of or pertaining to sexual activity with children, child pornography, child erotica, or access to or sexual interest in children.

4. Information, correspondence, records, documents, or other materials constituting evidence of human trafficking, commercial sex acts, or travel to and / or transportation of a minor with intent to engage in sexual activity, including records of payments to or for minors, hotel reservations and receipts, gas and restaurant receipts, GPS data, and Wi-Fi connections.

5. Any and all information and materials, in any format or medium, that concern email accounts, online storage, or other remote computer storage relevant to the above offenses.

6. Any information or materials that concern ownership and/or usage of the SUBJECT DEVICES, including:

   (a) Evidence of who used, owned, or controlled the SUBJECT DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

   (b) Evidence of software that would allow others to control the SUBJECT DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

   (c) Evidence of the lack of such malicious software.

(d) Evidence of the attachment to the SUBJECT DEVICES of other storage devices or similar containers for electronic evidence.

(e) Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the SUBJECT DEVICES.

(f) Evidence of the times the SUBJECT DEVICES were used.

(g) Records of or information about Internet Protocol addresses used by the SUBJECT DEVICES.

(h) Records of or information about the SUBJECT DEVICES' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

(i) Contextual information necessary to understand the evidence described in this attachment.

ATTACHMENT A

Property to Be Searched

This warrant applies to:

A. One (1) Black Apple Watch – Series 6, listed under HCSO property evidence number PE22-02303

B. One (1) Black Apple iPhone with SIM Card, listed under HCSO property evidence number PE22-02306

C. One (1) Black Google Android Phone with SIM Card, listed under HCSO property evidence number PE22-02304

D. One (1) Black Cricket Phone, listed under HCSO property evidence number PE22-02305

E. One (1) Black 1+ Phone, listed under HCSO property evidence number PE22-02307

F. One (1) Green Apple iPhone with SIM Card, listed under HCSO property evidence number PE22-02308 MOM

(collectively the SUBJECT DEVICES), held at the Hamilton County Sheriff's Office (HCSO), located at 6233 Dayton Blvd, Chattanooga, Tennessee, in the Eastern District of Tennessee.

This warrant authorizes the forensic examination of the SUBJECT DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED

All records, located within the SUBJECT DEVICES listed in Attachment A, that constitute contraband or evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 2422(b), **Coercion and enticement**; 2423(a), **Transportation with intent to engage in criminal sexual activity**, 2423(b), **Travel with intent to engage in illicit sexual conduct**, 2251(a) and (e), **Sexual exploitation of children** (production of child pornography); and 2252A(a)(1), (2), (5)(B) and (b), **Certain activities relating to material constituting or containing child pornography**; including:

1. Images or visual depictions of child pornography, as that term is defined in 18 U.S.C. § 2256(8).

2. Images and videos of child erotica (i.e., children engaged in sexually suggestive poses or settings that do not meet the definition of child pornography).

3. Information, correspondence, records, documents, or other materials constituting evidence of or pertaining to sexual activity with children, child pornography, child erotica, or access to or sexual interest in children.

4. Information, correspondence, records, documents, or other materials constituting evidence of human trafficking, commercial sex acts, or travel to and / or transportation of a minor with intent to engage in sexual activity, including records of payments to or for minors, hotel reservations and receipts, gas and restaurant receipts, GPS data, and Wi-Fi connections.

5. Any and all information and materials, in any format or medium, that concern email accounts, online storage, or other remote computer storage relevant to the above offenses.

6. Any information or materials that concern ownership and/or usage of the SUBJECT DEVICES, including:

   (a) Evidence of who used, owned, or controlled the SUBJECT DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

   (b) Evidence of software that would allow others to control the SUBJECT DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

   (c) Evidence of the lack of such malicious software.

(d) Evidence of the attachment to the SUBJECT DEVICES of other storage devices or similar containers for electronic evidence.

(e) Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the SUBJECT DEVICES.

(f) Evidence of the times the SUBJECT DEVICES were used.

(g) Records of or information about Internet Protocol addresses used by the SUBJECT DEVICES.

(h) Records of or information about the SUBJECT DEVICES' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

(i) Contextual information necessary to understand the evidence described in this attachment.

United States Department of Justice
Criminal Division

Child Exploitation and Obscenity Section
High Technology Investigative Unit

Subject: Technical Assistance Request – Investigation of Jonathan Salazar	
Examiner: Dero Tucker	**ACTS Number:** 202232407
Case Type: Child Exploitation	**Report Date:** December 23, 2022
Attachments: 6	**Page:** 1 of 3

ITEMS TO BE EXAMINED:

1. **"File system Extraction.zip"** is a Cellebrite full file system extraction of an Apple iPhone 11 with IMEI 352898116627242; created on September 27, 2022 by Digital Investigative Analyst (DIA) Dero Tucker.
2. **"File system Extraction.zip"** is a Cellebrite full file system extraction of an Apple iPhone 11 with IMEI 352910114869989; created on September 27, 2022 by DIA Dero Tucker.
3. **"EXTRACTION_BFU.zip"** is a Cellebrite Before First Unlock (BFU) extraction of a Google Pixel 2 XL with IMEI 358034089208059; created on September 21, 2022 by DIA Dero Tucker.

TECHNICAL ASSISTANCE REQUESTED:

Identify evidence of child exploitation offenses, Johnathan Salazar, and minor victims on seized evidence items.

FINDINGS:

ITEM 1: File system Extraction.ufd (Mint Green Apple iPhone 11)

1. **Facebook Messenger**
   Facebook Messenger is an application installed on mobile devices, such as Apple iPhones, that allow Facebook users to send chat messages, images, videos, and files to other Facebook users. The Facebook Messenger application also allow users to conduct voice and video calls. The Facebook Messenger application stored sent and received Facebook Messenger chat messages in the database file "lightspeed-100054029273079.db". This database file was located in the folder "/private/var/mobile/Containers/Shared/AppGroup/B081ED60-7EE2-46FC-A9E0-2B301278A176/".

   A review of the database file "lightspeed-100054029273079.db" identified the Facebook Messenger user account associated with this Apple iPhone 11 as "Margaret A Salazar" with email "margaretsalazar25@yahoo.com" and unique ID "100054029273079". Further review of the database file "lightspeed-100054029273079.db" identified Facebook Messenger chat messages on June 1, 2022 and June 2, 2022 between "Margaret A Salazar" and "Mary Alice Garcia" in which "Margaret A Salazar" sent the messages "You want go with me to Tennessee", "John went to puck up his gf", and "I don't trust that why I'm following him".

   Attachment 1 contains the database file "lightspeed-100054029273079.db". **Attachment 2** contains the extracted Facebook Messenger chat messages stored within the database file "lightspeed-100054029273079.db".

2. **Text Messages**
Apple devices, such as the Apple iPhone, stores a record of sent and received Short Message Service (SMS) messages, including Apple iMessages, in the database file "sms.db". The database file "sms.db" was located in the folder "/private/var/mobile/Library/SMS/". These text messages range between August 1, 2020 and June 2, 2022. A review of the database file "sms.db" identified text messages between the user of this Apple iPhone 11 with phone number "361-484-8091" and phone number "423-464-2610" on June 1, 2022. On June 1, 2022, phone number "423-464-2610" sent the message "Hi this is Kady" in which the user of this Apple iPhone 11 replies with the messages "Hi I'm John mom" and "I love you". Below is a snippet of subsequent conversations between The user of this Apple iPhone 11 with phone number "361-484-8091" and phone number "423-464-2610" on June 1, 2022.

From	To	Text	Time stamp (New York)
+14234642610	+13614848091	I wanted to make sure if it's ok if I sent you a screenshot of the life360 for you to download the right one and login and I can send the link to you if that's ok	6/1/2022 6:23:17 PM
+13614848091	+14234642610	Ok ty send me	6/1/2022 6:25:18 PM
+14234642610	+13614848091		6/1/2022 6:26:07 PM
+14234642610	+13614848091	Then once you get logged in it really ain't hard to get logged into and I can send you the link you just gotta do like one thing I'm pretty sure	6/1/2022 6:26:52 PM
+14234642610	+13614848091	It's the purple one	6/1/2022 6:27:05 PM
+13614848091	+14234642610	Ok	6/1/2022 6:27:42 PM
+14234642610	+13614848091	Let me know when you get logged into it so I can send you the link	6/1/2022 6:36:30 PM
+14234642610	+13614848091	Or if you need help getting logged into it	6/1/2022 6:36:45 PM
+13614848091	+14234642610	Ok	6/1/2022 6:36:52 PM
+14234642610	+13614848091	Join my Life360 Circle! Use my invite code EBB-KGO. Download the app here: https://i.lf360.co/TL5u7hG7vqb	6/1/2022 7:24:08 PM
+14234642610	+13614848091	That's the link to join the group	6/1/2022 7:24:23 PM
+13614848091	+14234642610	Can you send me a pic of you	6/1/2022 7:26:48 PM

Attachment 3 contains the database file "sms.db". **Attachment 4** contains the extracted text messages stored within the database file "sms.db".

3. **DCIM Folder**
The folder "/mobile/Media/DCIM/" and its subfolders contains 1,240 images and videos with file creation dates ranging between August 2, 2020 and June 2, 2022. Some of the images with creation dates of June 1, 2022 and June 2, 2022 appear to be screenshots of the application Life360, such as "IMG_8714.PNG", "IMG_8725.PNG", and "IMG_8747.PNG". Life360 is an application that allow users to share their location, alert, and communicate with other approved Life360 users. In some of the screenshots, the names "John" and "Kady" can be identified. The contents of the folder "DCIM" and its subfolders are included in **Attachment 5**. **Attachment 6** contains the file attributes for the images and videos stored in the folder "DCIM" and its subfolders.

ITEM 2: File system Extraction.ufd (Black Apple iPhone 11)

Additional evidence regarding Jonathan Salazar or minor victims were not identified on this evidence item. This device appear to be unused or recently setup.

ITEM 3: EXTRACTION_BFU.zip (Google Pixel XL)

Additional evidence regarding Jonathan Salazar or minor victims were not identified on this evidence item. The passcode to gain access to this device is unknown.

DERO TUCKER Digitally signed by DERO TUCKER Date: 2022.12.23 11:28:02 -05'00'

(Signature of examiner) *(Date)*

JAMES FOTTRELL Digitally signed by JAMES FOTTRELL Date: 2022.12.23 10:41:55 -05'00'

(Signature of reviewer) *(Date)*

CASE NUMBER
TT05PS22TT0002

CASE OPENED
6/9/2022

CURRENT CASE TITLE
Kidnapping of 15 YO Girl and Arrest of Johnathan Lucino...

REPORT TITLE
Digital Forensics Report

REPORTED BY
Steven Burns
NO TITLE FOUND

APPROVED BY
Arturo Napolitano
SPECIAL AGENT

DATE APPROVED
12/19/2022

SYNOPSIS

This report serves to document the digital forensics review of digital devices involved in a child abduction.

DETAILS OF INVESTIGATION

INTRODUCTION:

The digital devices detailed below were reviewed by Homeland Security Investigations (HSI) Computer Forensics Analyst (CFA) Steven Burns upon request of Special Agent (SA) Antonio Escobar of HSI. The devices were provided by Detective (DET) Jason Maucere of the Hamilton Country Sheriff's Office (HCSO), TN.

EVIDENCE:

FPF No.	**2022200800001201**
LINE ITEM 001:	**MOTOROLA CELLULAR DEVICE – MODEL: XT2163DL**
MAKE	MOTOROLA
MODEL	MOTO G PURE (XT2163DL)
IMEI	356 676 309 945 043
VERSION	ANDROID 11

FPF No.	**2022200800001401**
LINE ITEM 001:	**GOOGLE PIXEL 2 XL**
Make	Google
Model	Pixel 2 XL G011C

IMEI	UKN
LINE ITEM 002:	**APPLE IPHONE 11 (GREEN)**
Make	Apple
Model	iPhone 11 (A2111)
IMEI	352 898 116 627 242
LINE ITEM 003:	**APPLE IPHONE 11 (BLACK)**
Make	Apple
Model	iPhone 11 (A2111)
IMEI	352 910 114 860 989
LINE ITEM 004:	**CRICKET ICON 2**
Make	Cricket
Model	Icon 2 (U325AC)
IMEI	866 530 040 304 296
LINE ITEM 005:	**APPLE WATCH (SERIES 6)**

Make	Apple
Model	Apple Watch (Series 6)
LINE ITEM 006:	**ONEPLUS 8 5G**
MAKE	ONEPLUS
MODEL	ONEPLUS 8 5G UW (IN2019)
IMEI	869 904 040 385 430

SEARCH AUTHORITY AND CUSTODY:

On 06-24-2022, CFA Burns received LINE ITEM 001 (FPF No. 2022200800001201) from DET Maucere of the HCSO accompanied by a consent form, signed by the device owner, authorizing the search of this device.

On 08-22-2022, CFA Burns received LINE ITEM 001-006 (FPF No. 2022200800001401) from DET Maucere of the HCSO accompanied by a search warrant authorizing the search of these devices.

On 09-15-2022, CFA Burns sent LINE ITEM 001-003 (FPF No. 2022200800001401) to the Department of Justice (DOJ), Child Exploitation and Obscenity Section (CEOS), High Technology Investigative Unit (HTIU) because data acquisition was not supported locally for these devices.

AQUISITION:

Mobile device data was acquired utilizing the software program Cellebrite UFED 4PC. Mobile devices are connected to a computer running UFED 4PC and the software facilitates the acquisition of mobile device data at the logical, file system, and physical levels through various methods. The acquired data can be manually examined or imported into forensic software for processing and analysis. An APK downgrade process was coupled with the Android Backup to acquire additional application data.

FPF No.	**2022200800001201**

LINE ITEM 001	**MOTOROLA CELLULAR DEVICE - MODEL: XT2163DL**
Acquisition Software	Cellebrite UFED 4PC (7.54.0.444)
Acquisition Type	Advanced Logical, File System (Android Backup)
FPF No.	**2022200800001401**
LINE ITEM 004	**CRICKET ICON 2**
Acquisition Software	Cellebrite UFED 4PC (7.57.0.13)
Acquisition Type	Advanced Logical, File System (Android Backup)
LINE ITEM 006	**ONEPLUS 8 5G**
Acquisition Software	Cellebrite UFED 4PC (7.57.0.13)
Acquisition Type	Advanced Logical, File System (Android Backup)

No data acquisition was conducted for the below devices.

FPF No.	**2022200800001401**
LINE ITEM 001	**GOOGLE PIXEL 2 XL**

Local capabilities did not support data acquisition. Sent to CEOS-HTIU.	
LINE ITEM 002	**APPLE IPHONE 11 (GREEN)**
Local capabilities did not support data acquisition. Sent to CEOS-HTIU.	
LINE ITEM 003	**APPLE IPHONE 11 (BLACK)**
Local capabilities did not support data acquisition. Sent to CEOS-HTIU.	
LINE ITEM 005:	**APPLE WATCH (SERIES 6)**
Local capabilities did not support data acquisition.	

PROCESSING:

The software programs below were utilized to process the acquired device data.

Cellebrite Physical Analyzer was utilized for the processing and analysis of the acquired device data. All processed data was exported in multiple report formats from Cellebrite Physical Analyzer.

Magnet AXIOM was utilized for the processing and analysis of the acquired device data.

Griffeye Analyze DI Pro was utilized for the processing and analysis of media items (i.e., images and videos). Media items of investigative interest were exported in multiple report formats from Griffeye Analyze DI Pro.

Additional processing information is included in the software reports that were provided to the case agent.

EXAMINATION RESULTS:

The results below are only a summary, for full details refer to the software reports provided to the case agent.

FPF No. 2022200800001201

LINE ITEM 001 MOTOROLA CELLULAR DEVICE - MODEL: XT2163DL

Sexually explicit Snapchat messages were found between the device owner (User ID: efe07786-66c2-4371-abe5-b8e6de2ce302) and a contact with the username of "kade_blake22" and a display name of "John" (User ID: 598c6b00-c766-417b-a894-05a5200cdb27). The source of these messages is the conversation_message table of the arroyo.db located in the backup of the Snapchat application (*apps/com.snapchat.android/db/arroyo.db*). This database table contains chat communications sent and received from within the Snapchat application. These communications could be text data and /or include attachments, such as images, videos, or voice messages. The Snapchat account "kade_blake22" is associated with *LINE ITEM 006 (2022200800001401)*.

Sexually explicit text messages were found between the device owner and a contact labeled "Johnny" with the phone number of (361) 676-4721. Additionally, phone calls were found between the device owner and "Johnny". This phone number is associated with *LINE ITEM 006 (2022200800001401)*.

FPF No. 2022200800001401

LINE ITEM 004 CRICKET ICON 2

Phone calls were found between the device owner and a contact labeled "John" with the phone number of (361) 676-4721. This phone number is associated with *LINE ITEM 006 (2022200800001401)*.

LINE ITEM 006 ONEPLUS 8 5G

Sexually explicit snapchat messages were found between the device owner (User ID: 598c6b00-c766-417b-a894-05a5200cdb27) and a contact with the username of "kdefur6" and a display name of "Kady" (User ID: efe07786-66c2-4371-abe5-b8e6de2ce302). The source of these messages is the conversation_message table of the arroyo.db located in the backup of the Snapchat application (apps/com.snapchat.android/db/arroyo.db). The Snapchat account "kdefur6" is associated with *LINE ITEM 004 (2022200800001401)*.

Media files were found within the backup of the Snapchat application with content that appears to show the identified victim. 18 images (4 unique) and 7 unique videos were found that appear to contain sexually explicit content. Media files being present at this location is indicative that the files were sent or received by the the associated Snapchat account (598c6b00-c766-417b-a894-05a5200cdb27). *Source: apps|com.snapchat.android|f|native_content_manager|com.snap.file_manager_3_SCContent_598c6b00-c766-417b-a894-05a5200cdb27*

Sexually explicit text messages were found between the device owner and a contact labeled "Kady MI AMOR " with a phone number of (423) 464-2610. Additionally, phone calls were found between the device owner and "Kady MI AMOR ".

A contact was found labeled "Mom" with the phone number of (361) 489-9798. This phone number is associated with *LINE ITEM 004 (20222008000014O1)*.

ADDITIONAL INFORMATION:

These reports were provided to the case agent. If any additional items are found that could be of investigative interest contact the assigned analyst for interpretation and/or verification.

CONCLUSION:

Supplemental information may be available upon request. If, after reviewing this report, you require additional information or further computer forensics support contact the assigned analyst or case agent.